Probabilistic Bounds on the Impact of Potential Data Integrity Attacks in Microgrids

Hao Jan Liu, Hyungjin Choi, Paprapee Buason, and Alfonso Valdes *
Department of Electrical and Computer Engineering and Information Trust Institute, University of Illinois at Urbana-Champaign
Emails: {haoliu6,hjchoi12,buason2,avaldes}@illinois.edu

Abstract

Microgrids are being increasingly adopted in electric power distribution systems to facilitate distributed energy resource integration and to provide resilient operations. Modern microgrids rely on sophisticated cyber communications and controls to maintain stable operation. Attacks on this cyber infrastructure can cause the system to undertake a potentially destabilizing control action. In this work, we present the results of a reachability analysis in which we determine whether a potential attack vector can result in actions that make an unstable state "reachable" in some time interval from the current state. Specifically, our analysis must be executed on a timescale that heads off the destabilizing system states due to malicious attacks. To that end, we propose a sensitivity analysis that assesses the worst-case impact of attack scenarios of interest while identifying reachable unstable states in the required time budget. This concept can be used to develop a tool to support DER control decisions under adverse conditions. Numerical tests are provided to validate the effectiveness of the attack reachability analysis.

1. Introduction

Microgrids (MGs) are increasingly being introduced in distribution networks to promote the integration of distributed energy resources (DERs) and elastic loads, coupled with a significant modernization of metering, computing, and communication infrastructure [1]. Meanwhile, MGs' ability to operate in two modes, i.e., islanded and grid-connected, further enhances system reliability and resiliency against disturbances in the bulk power networks [2].

However, deployment of MGs requires a hierarchical control framework that includes sensors, actuators, and other intelligent control components communicating over a cyber network, to perform functions such as the distributed voltage and frequency controls in [3–6]. Consequently, there are growing concerns about the stable and reliable operation of MGs where vulnerability to cyber attacks on communication, measurement, and control systems poses significant threats; see, e.g., [7–11] and references therein. Such attacks are not hypothetical, as evidenced by recent cyber-induced outages in Ukrainian power systems [9]. Accordingly, there is a pressing need to develop an online analytic tool to continuously monitor for and predict the potential impact of cyber attacks on MGs while offering preventive countermeasures. Such a tool would be important in providing decision support for DER coordination under adversarial environments.

There have been active research efforts to address the cybersecurity concerns with MGs. Real-time simulators such as RTDS and testbeds have been used to analyze the impact of malicious cyber events and test real-time hardware-in-the-loop systems [12–14]. In addition, prior work in [10, 15, 16] has developed defense frameworks and countermeasures against malicious attacks. Nonetheless, prior efforts have fallen short of continuously monitoring and predicting potential cybersecurity impacts. Accordingly, repeated numerical simulations, such as Monte Carlo methods, have been proposed to analyze the impact of cyber attacks on MG dynamic states, e.g, angle and frequency [17–20]. From a practical point of view, those numerical simulations are computationally burdensome when all possible attack scenarios are considered. To the

*The work described here was performed with funding from the Dept. of Energy (DOE) under Cooperative Agreement DE-OE0000831, under subcontract to ABB US Corporate Research Center. The views expressed are those of the authors. This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

URI: https://hdl.handle.net/10125/59787
ISBN: 978-0-9981331-2-6

best of our knowledge, none of the prior work can be implemented in a real-time setting that reflects the physical structure of MGs directly related to the dynamical stability of the system. Thus, we aim to improve the computational feasibility of the analysis while facilitating the protection of systems from cyber attacks in a nearly online fashion.

Aligned with the need for comprehensive methods to improve the cybersecurity of MGs, we propose a sensitivity-based reachability analysis to quantify the impact of cyber attacks on measurement and control commands to transient stability of MGs. This study provides the worst-case upper and lower bounds on dynamic states (voltage and frequency) under a specified attack. By *reachability*, we mean that an unstable state is "reachable" from the current state in the presence of particular attacks. Henceforth, our analysis may be utilized to predict any potential fault conditions induced by violating the safety limits of protection systems such as relays. The core of our proposed method is threefold. First, we adopt the reduced-order model to describe the dynamics of droop-controlled DER interface converters (DICs) [21] and DC power-flow assumptions [22] to speed up the computation time of our analysis. Next, sensitivity analysis is introduced to approximate the coupling among dynamic states and attack inputs. Last but not least, we model the attack on the measurement as a random variable for which sensitivity analysis is executed to estimate the worst-case bounds on all possible variations in dynamical states. Overall, the reachability analysis will provide the probabilistic estimation bounds in a nearly online fashion to quantify the potential impact of cyber attacks. Therefore, our approach contributes a systematic solution to estimating the worst-case impact of cyber attacks on the dynamical behavior of MGs without applying repeated time-domain simulations or complex mathematical algorithms. In addition, the sensitivity evaluation can provide crucial cybersecurity information to counter attacks on cyber-physical MG networks by facilitating DER coordination decisions.

The remainder of this paper is as follows. Sec. 2 presents the modeling of MGs, while Sec. 3 defines an attack scenario based on corruption of the voltage measurement and then describes sensitivity analysis of attacks on dynamical states. In Sec. 4, we describe how we validate the effectiveness of the proposed reachability analysis by performing Monte Carlo simulation. We conclude in Sec. 5.

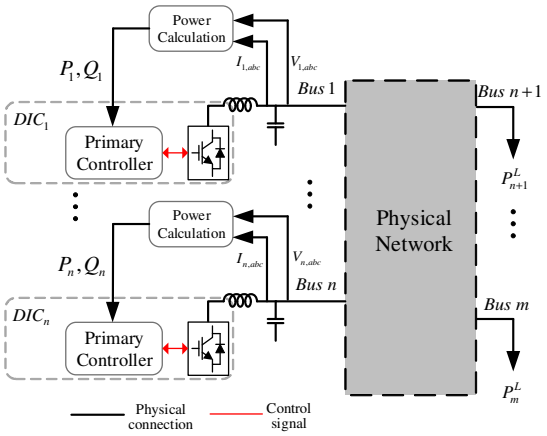

Figure 1. A cyber-physical MG network with DICs, in which $V_{i,abc}$ and $I_{i,abc}$ are the instantaneous three-phase voltage and current measurement sample values, respectively.

2. Modeling of a Microgrid

Given an islanded MG that includes all grid components, such as DICs, loads, and lines, as depicted in Fig. 1, we represent an MG with a connected graph $(\mathcal{N}_M, \mathcal{E}_M)$. Without loss of generality, the set $\mathcal{N}_M$ consists of the subsets $\mathcal{N}_D := \{1, \cdots, n\}$ and $\mathcal{N}_L := \{n+1, \cdots, m\}$, representing the DIC and load buses, respectively. In addition, the line segments connecting the buses are represented by the set $\mathcal{E}_M$. Per bus-i, V_i and θ_i are defined as the voltage magnitude and phase angle, respectively, and $V_{i,abc}$ is the three-phase instantaneous voltage sample value. Moreover, we let P_i (Q_i) represent the active (reactive) power injection from DIC_i, while P_i^M denotes its active power rating, and P_i^L (Q_i^L) is the active (reactive) power demand of the i^{th} load bus. For notational convenience in the rest of the paper, the frequency deviation is represented by $\omega_i := (\dot{\theta}_i - \omega_{\text{ref}})$, where $\dot{\theta}_i := d\theta_i/dt$ is the frequency, and ω_{ref} is the reference frequency set-point. To facilitate the ensuing reachability analytics, we also make the following assumptions:

AS 1. *The power lines are short, so line loss is negligible.*

AS 2. *The angular difference $(\theta_i - \theta_j), \forall i, j \in \mathcal{E}_M$ is small.*

AS 3. *Each bus voltage magnitude V_i is fixed at near unity (expressed as per unit).*

AS 4. *The active power demand $P_i^L, \forall i \in \mathcal{N}_L$ is constant during each control interval.*

AS 5. *All possible load variations under the isolated MG are supported by DICs without violating the active*

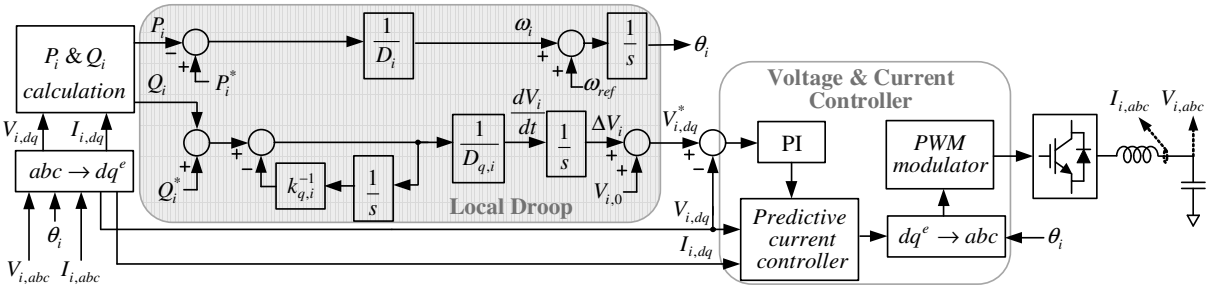

Figure 2. The figurative control diagram representation for an individual DIC$_i$.

power rating limits of the DICs.

Assumption 1 is often adopted in the MG literature; see, e.g., [3, 10, 11, 23, 24]. This assumption can be justified because of the short power lines in MGs. Thus, line losses are negligible compared to line flows. In addition, one can assume that all lines have a uniform homogeneous resistance-to-inductance ratio, and thus we can recover a lossless model by performing a linear transformation to decouple lossy and lossless injections; see, e.g., [25, Remark 1]. Regarding angular difference among buses in Assumption 2, these values should be small due to the proximity of buses within a MG. As for the constant voltage in Assumption 3, it can be ensured through the fast inner voltage control loop of DICs, see, e.g., [26]. Together with the voltage-droop controller, the DIC output voltage can track the voltage reference setpoint by managing DICs' reactive power output at a much faster time-scale than that of the frequency controller. Earlier work in [3, 11, 24, 27] has supported such a time-scale separation between frequency and voltage dynamics. We also assume that some active or passive shunt compensators or some control mechanisms exist throughout the network to maintain a healthy voltage profile. Henceforth, the voltage magnitude at each bus can be presumed constant at nearly unity at the timescale of the frequency control design. The constant power demand in Assumption 4 comes from the design of the proposed controller to be sufficiently fast to stabilize the system in response to a load disturbance before the next disturbance occurs. Finally, Assumption 5 can be satisfied through careful system planning at the MG deployment stage. To sum up, we consider only the reachability analysis of the frequency control design while neglecting the voltage arguments from all related functions. Although we adopt those assumptions to facilitate the ensuing analysis, the numerical test in Sec. 4 will be based on a realistic lossy MG model with fully detailed DIC dynamics that includes the inner voltage and outer current control loops to showcase the effectiveness of the proposed analysis.

2.1. Frequency-Based Active Power Control

For an islanded MG, each DIC$_i$ behaves like a voltage source by regulating V_i and θ_i via the feedback droop-based control; see, e.g., [3, 24, 28]. Fig. 2 depicts a high-order converter model consisting of fast inner- and outer-control loops and frequency- and voltage-droop controllers. As the converter's internal dynamics are much faster than those of the system states, it has been shown in [21] that ignoring the former would neither compromise the modeling fidelity nor affect the stability conditions of the latter at the time-scale of power system analysis. Accordingly, we adopt the reduced-order model (see, e.g., μROm2 in [21]) in this paper. Using Assumption 3, one can derive the reduced-order dynamic equations per DIC$_i$ from a fully detailed converter model by ignoring the voltage dynamics, as given by

$$\frac{1}{\tilde{\omega}_i}\frac{d\tilde{P}_i}{dt} = -\tilde{P}_i + P_i, \tag{1a}$$

$$D_i\omega_i = P_i^M - \tilde{P}_i, \tag{1b}$$

where $\tilde{\omega}_i > 0$ is the cut-off frequency of the i^{th} low-pass filter, and $\tilde{P}_i$ is the filtered active power injection of DIC$_i$. The effect of the low-pass filter is captured by (1a), while the frequency droop control design is governed by (1b). Differentiating (1b) from (1a) and substituting the result into (1a), we have the following simplified dynamics of the droop-controlled DIC$_i$:

$$\frac{d\omega_i}{dt} = -\tilde{\omega}_i\omega_i + \frac{\tilde{\omega}_i}{D_i}(P_i^M - P_i), \forall i \in \mathcal{N}_D. \tag{2}$$

As detailed below in Sec. 3, the sensors at DIC$_i$ that measure active power injection P_i are considered to be potentially vulnerable to malicious attacks. In addition, note that the frequency deviation ω_i at steady-state is a nonzero value unless $P_i^M = P_i, \forall i \in \mathcal{N}_D$. Adjusting the frequency back to the reference set-point requires an additional control layer (i.e., a secondary frequency

control design [3, 10, 24, 27]) and is beyond the scope of this work.

2.2. Load Model

Power loads usually depend on both bus voltage (which is assumed constant under Assumption 3) and frequency. Without loss of generality, the load dynamics can be represented by either a dynamics-free constant ZIP or a frequency-dependent load model. The former consists of impedance (i.e., resistor and inductor), current source, and real and reactive power load (i.e., PQ load), while the latter is a frequency-sensitive load, in which the power consumption increases linearly with the frequency deviation ω_i and its velocity $\dot{\omega}_i$, e.g., a motor-type load [29]. In this work, all loads, unless specifically stated otherwise, are assumed to be of the frequency-sensitive type. Therefore, the dynamics is given by

$$J_i\dot{\omega}_i + D_i\omega_i = -P_i^L - P_i, \forall i \in \mathcal{N}_L, \tag{3}$$

where $J_i > 0$ and $D_i > 0$ represent the physical inertia and damping constant associated with the i^{th} load bus, respectively [30].

2.3. DC Power Flow

Real and reactive power-flow balance at bus $i \in \mathcal{N}_M$ is described by the following nonlinear algebraic equations:

$$0 = \sum_{j\in\mathcal{N}_i} V_iV_j\left(G_{ij}\cos(\theta_i-\theta_j) + B_{ij}\sin(\theta_k-\theta_j)\right) - P_i, \tag{4a}$$

$$0 = \sum_{j\in\mathcal{N}_i} V_iV_j\left(G_{ij}\sin(\theta_i-\theta_j) - B_{ij}\cos(\theta_k-\theta_j)\right) - Q_i, \tag{4b}$$

where $\mathcal{N}_i := \{j \,|\, (i,j) \in \mathcal{E}_M\}$ denotes the set of neighbor buses of bus i, and B_{ij} (G_{ij}) is the susceptance (conductance) of the line between bus i and bus j. Using Assumptions 1–3 and concatenating all scalars into vectors, one can simplify (4) to the well-known DC power flow, as given by

$$\mathbf{0} = \mathbf{B}\boldsymbol{\theta} - \mathbf{P}. \tag{5}$$

By solving (5), we have the explicit solution for the bus angle

$$\boldsymbol{\theta} = \mathbf{B}^{-1}\mathbf{P}, \tag{6}$$

which, together with (2) and (3), gives the power system differential and algebraic equations.

3. Reachability Analysis

In this section, given attacks on measurement and control inputs, we develop a methodology for reachability analysis on dynamical states. We first describe the data integrity attack model and then propose a linear sensitivity analysis to approximate the coupling among dynamic states and attack inputs. All possible variations of the dynamic state due to attacks can be effectively determined by a linear transformation that uses the sensitivity analysis.

3.1. Data Integrity Attacks

Under the assumption that the attacker can access some of the sensors and communication network to alter the measurement data or control commands, the dynamics of the MG network model with two-state DER dynamics (e.g., angle and frequency) is described by a set of differential equations as follows:

$$\frac{dx_i}{dt} = f_i(\mathbf{x}, \hat{\mathbf{u}}), \quad \text{for } i = 1, \ldots, 2m, \tag{7}$$

where $\mathbf{x} := [\boldsymbol{\theta}; \boldsymbol{\omega}] \in \mathbb{R}^{2m}$ represents the dynamic states (i.e., angle and frequency), and $\hat{\mathbf{u}} \in \mathbb{R}^{\ell}$ collects the attacked control and measurement inputs. Note that our MG model does not contain any internal buses that are without any generations or loads. For a more general setting in which we have algebraic equations coupling power-flow balance in the internal buses, we can also remove those buses by performing network reduction techniques such as Kron reduction and recover the differential equations in (7) [31].

Without loss of generality, we define a *data integrity attack* as a malicious modification of an original signal $\mathbf{u}$ by the attack input $\boldsymbol{\xi}$ such that

$$\hat{u}_j = (1 + \xi_j) \cdot u_j, \quad \text{for } j = 1, \ldots, \ell. \tag{8}$$

Note that an uncorrupted input signal $\hat{u}_j$ is equivalent to setting $\xi_j = 0$. The following example explains the dynamic equations with attacks on the instantaneous voltage measurement sample $V_{i,abc}$ for a simple two-bus system, as shown in Fig. 3.

Example 1. *Fig. 3 illustrates the aforementioned attack model for the single-line per unit diagram of the two-bus power system. To better explain the impact of corrupted measurements on dynamic states, we simplify the network model by only considering a DIC at bus* 1 *and a constant PQ load at bus* 2*, resulting in fewer dynamic states. Nominal parameters and inputs are* $V_1 = 1$, $V_2 = 1$, $X_L = 0.15$, $P_2^L = 0.2$, $Q_2^L = 0.1$, $P_1^M = 0.3$, $D_1 = 50\,[\text{s/rad}]$, *and*

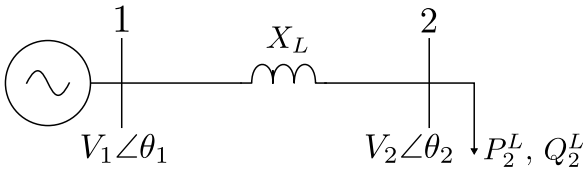

Figure 3. Two-bus system (from Example 1) with DER at bus 1 and a constant PQ load at bus 2.

$\tilde{\omega}_1 = 31.4\,[\mathrm{rad/s}]$. *All quantities are per-unit unless otherwise explicitly specified. We assume that the voltage measurement at bus* 1 *is corrupted (as denoted by* $\hat{V}_1$*), so that the attacker alters the true measurements by the multiplicative scale factor* ΔV_1*, i.e.,*

$$\hat{V}_1 = (1 + \Delta V_1) \cdot V_1,$$

and thus corrupts the original droop-based frequency control scheme. Similar analysis can be applied to droop-based voltage control design [32]. Note that the multiplicative attack in (8) *on* $V_{1,abc}$ *is equivalent to scaling of the phasor voltage magnitude by* ΔV_1.

Accordingly, the network dynamic equation based on (7) *becomes*

$$\begin{aligned}\frac{d\omega_1}{dt} &= f_1(\mathbf{x}, \hat{\mathbf{u}}) \\ &= -\tilde{\omega}_1\omega_1 + \frac{\tilde{\omega}_1}{D_1}\left(P_1^M - (1+\Delta V_1)\, P_2^L\right). \end{aligned} \quad (9)$$

Note that (9) *is a result of DC power flow assumptions under which* $\theta_2 = \theta_1 - P_2^L X_L$*. For this simple case, we have* $\mathbf{x} = \omega_1$ *and* $\boldsymbol{\xi} = \Delta V_1$. ■

Remark 1 (Attack Generalizations)**.** In this study, we model the attack as a malicious multiplier that scales the true measurement as shown in (8). Nonetheless, our method is not limited to this specific attack and can be designed to account for various types of attacks, such as false data injection, in which attack vectors are added to the original measurement.

3.2. Linear Approximation and Dynamics of Sensitivity Variables

Following the dynamic equation of the MG network in (7), we let $\mathbf{x}(t, \boldsymbol{\xi})$ be the solution of dynamic states under the attack vector $\boldsymbol{\xi}$. Hence, the first-order linear approximation of dynamic states in terms of $\boldsymbol{\xi}$ is

$$\mathbf{x}(t, \boldsymbol{\xi}) \approx \mathbf{x}(t, \mathbf{0}) + \boldsymbol{\Phi}\boldsymbol{\xi}, \quad (10)$$

where $\mathbf{x}(t, \mathbf{0})$ is the nominal solution without attacks, and the matrix $\boldsymbol{\Phi} \in \mathbb{R}^{2m\times\ell}$ with its entry $\phi_{ij} := \frac{\partial x_i}{\partial \xi_j}$ accounts for the sensitivity of dynamic states in terms of the attack vector $\boldsymbol{\xi}$. Based on our previous work in [33], we can determine $\boldsymbol{\Phi}$ at each instance of time by solving the following differential equations (see Appendix A for details):

$$\frac{d}{dt}\boldsymbol{\Phi} = \boldsymbol{\Lambda}_{\mathbf{x}}\Big|_{\boldsymbol{\xi}=\mathbf{0}}\boldsymbol{\Phi} + \boldsymbol{\Lambda}_{\boldsymbol{\xi}}\Big|_{\boldsymbol{\xi}=\mathbf{0}}, \quad (11)$$

where $\boldsymbol{\Lambda}_{\mathbf{x}}$ and $\boldsymbol{\Lambda}_{\boldsymbol{\xi}}$ are the Jacobian of $\mathbf{f}$ in terms of $\mathbf{x}$ and $\boldsymbol{\xi}$, respectively. As our MG model does not contain any internal buses, we do not have algebraic terms or algebraic sensitivity equations corresponding to the dynamics of internal buses. We refer readers to [33] for cases in which we included algebraic terms to incorporate the effectiveness of the attack on power-flow balance in the internal network. By solving (11) together with the original dynamic equations in (7) for $\boldsymbol{\xi} = \mathbf{0}$ at each time t, we would obtain the value of $\mathbf{x}(t, \mathbf{0})$ as well as the time-varying sensitivity matrix $\boldsymbol{\Phi}$.

The following example depicts the linear approximation of a state and the formulation of sensitivity equations for the two-bus system continued from Example 1.

Example 2 (Example 1 continued)**.** *The matrix* $\boldsymbol{\Phi}$ *in* (10) *for the linear approximation of the dynamic state* $\mathbf{x}$ *in terms of the attack* $\boldsymbol{\xi}$ *is given by*

$$\boldsymbol{\Phi} = \frac{\partial\omega_1}{\partial\Delta V_1}. \quad (12)$$

Thus, the nominal solution for the state is determined by solving (9) *under* $\boldsymbol{\xi} = \mathbf{0}$*. Based on the formulation of sensitivity equations* (11)*, we obtain the relevant matrices as follows.*

$$\boldsymbol{\Lambda}_{\mathbf{x}}\Big|_{\boldsymbol{\xi}=\mathbf{0}} = -\tilde{\omega}_1, \quad \boldsymbol{\Lambda}_{\boldsymbol{\xi}}\Big|_{\boldsymbol{\xi}=\mathbf{0}} = -\frac{\tilde{\omega}_1 P_2^L}{D_1}.$$

We can calculate the sensitivity matrix $\boldsymbol{\Phi}$ *by solving* (11)*, and we can subsequently complete the linear approximation in* (10)*.* ■

As detailed subsequently, we propagate the attack $\boldsymbol{\xi}$ drawn from some probability distribution functions to estimate the probabilistic bounds on all possible variations of $\mathbf{x}(t, \boldsymbol{\xi})$ due to the attack $\boldsymbol{\xi}$.

Remark 2 (Approximation Errors)**.** Neglecting the higher-order terms leads to an approximation error in (11). It is possible to improve accuracy at the cost of additional computational burden by incorporating such higher-order terms, e.g., 2nd-order and mixed-sensitivity terms as discussed in [33]. That enhancement is beyond the scope of this paper and will be a future research direction.

3.3. Probabilistic Worst-Case Bounds on Dynamic States

We describe the jth attack, ξ_j, as a probabilistic random variable with normal distribution, i.e., $\xi_j \sim \mathcal{N}(0, \sigma_j^2)$, and individual attacks are mutually independent. Without loss of generality, an offline comprehensive study of all possible undetectable attack scenarios is assumed and thus justifies the probabilistic attack model. Then, based on (10), the ith state under the attack, $x_i(t, \boldsymbol{\xi})$, also follows a normal distribution with a mean value of $x_i(t, \mathbf{0})$ and a variance given by the sum of variances of $\boldsymbol{\xi}$ scaled by sensitivity variables, $\{\phi_{ij}\}_{j=1}^{\ell}$, i.e.,

$$x_i(t, \boldsymbol{\xi}) \sim \mathcal{N}\left(x_i(t, \mathbf{0}), \sum_{j=1}^{\ell} \phi_{ij}^2 \sigma_j^2 \right), \qquad (13)$$

which provides normally distributed worst-case bounds on the state x_i for the given attack $\boldsymbol{\xi}$. The following example demonstrates probabilistic worst-case bounds on dynamic states for the two-bus power system continued from Examples 1 and 2.

Example 3 (Examples 1 and 2 continued)**.** *In this example, the multiplicative attack $\boldsymbol{\xi}$ is described in terms of normally distributed random variables with zero mean values,*

$$\boldsymbol{\xi} = \Delta V_1 \sim \mathcal{N}(0, \sigma_1),$$

with standard deviations $\sigma_1 = 5$. We let the initial condition at $t = 0$ be $\omega_1(0) = 377.9991$ [rad/s] disturbed from the normal operating point. Accordingly, the worst-case bounds on the dynamic state are determined from (13) *by calculating $\mathbf{x}(t, \mathbf{0})$ and $\boldsymbol{\Phi}$ at each time t in Examples 1 and 2. The result is shown in Fig. 4. Red and blue curves show the estimated worst-case upper and lower bounds, respectively. Each curve indicates confidence levels of 99.7%, 95%, and 68% around the nominal trajectory denoted by black dotted lines. We verified the result via repeated time-domain simulations (denoted by green lines) for 100 randomly sampled attack values drawn from the normal distribution.*

Remark 3 (Scalability)**.** Thanks to Assumptions 1–5, the reduced-order DIC models introduced in Sec. 2, and the probabilistic attack description in (13), the proposed reachability analysis shows computational advantages over prior solutions while maintaining fair accuracy, and thus it can be adopted for larger MGs. As a comparison with [33] regarding scalability, the full MG dynamics is simplified to an ordinary differential equation (2), while the worst-case bounds are described by probabilistic distributions that do not resort to convex optimization. As detailed in the following section, our approach would significantly improve the scalability of the proposed method.

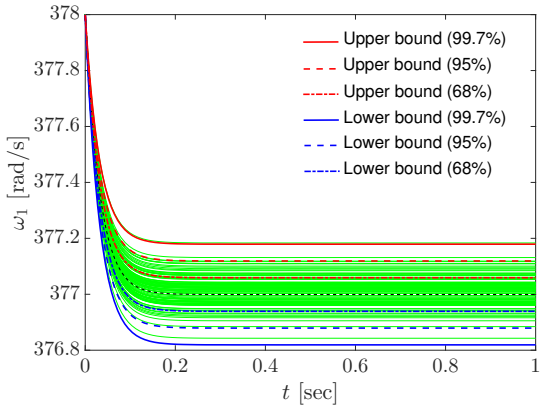

Figure 4. Worst-case bounds on the dynamic state $\mathbf{x}$ for the two-bus system (from Examples 1–3). Red and blue curves show the estimated worst-case upper and lower bounds, respectively, with different confidence levels, i.e., 99.7%, 95%, and 68%, around the nominal trajectory denoted by the black dotted lines. In addition, 100 repeated time-domain simulations, denoted by green lines, are also plotted to verify the effectiveness of the reachability analysis.

4. Numerical Tests

We have showcased the application of our proposed approach to quantify the impact of attacks on measurements based on the reachability analysis outlined in Sec. 3. We now consider a more realistic lossy MG model composed of three DICs governed by the droop-controlled scheme in the low-voltage distribution network. Fig. 5 provides a one-line diagram of the MG model under investigation. The system reference frequency $\omega_{\text{ref}} = 377 \text{ rad} \cdot \text{s}^{-1}$. The local control in the primary level works with a sampling rate of 20 kHz, which is needed to maintain a good output power quality, e.g., minimal frequency harmonics. For ease of observation, we set the rating of all DICs to the same value of 2 kW while fixing the droop gain uniformly as $50 \text{ kW} \cdot \text{s} \cdot \text{rad}^{-1}$. The dynamic load at bus 4 has the inertia constant $J_4 = 0.005 \text{ s} \cdot \text{rad}^{-2}$, the damping constant $D_4 = 10 \text{ s} \cdot \text{rad}^{-1}$, and the nominal apparent power demand $S_4 = 1.5 \text{ kW} + \text{j}0.525 \text{ kvar}$. Meanwhile, the MG is warm-started and initially operated at steady-state. In addition, the

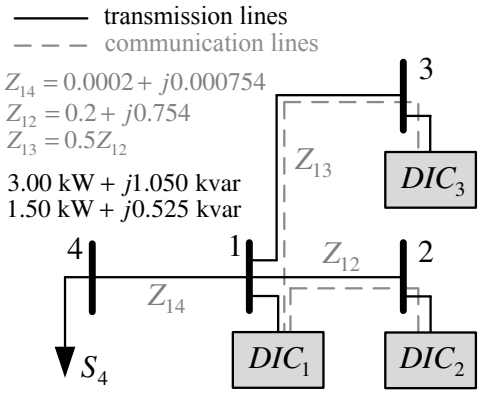

Figure 5. One-line diagram of the MG model for the numerical demonstration of our proposed method. Three droop-controlled DICs are connected to one load through the low-voltage distribution network.

probabilistic worst-case bounds are estimated at the beginnings of successive intervals of 2 seconds(s), at which times all parameters, including load demands and attack distribution, are known and remain constant during the time interval. Last, we introduce a 100% load increase at $t = 2$ s to further evaluate the effectiveness of the proposed analysis. Physical details of the MG, including inner-voltage and outer-current control loops and pulse width modulation emulation, are included and implemented in MATLAB Simulink®.

As for the reachability analysis, the dynamics of DICs are described by the simplified model as shown in (2). Dynamical states, including phase angles and frequencies of all DERs, are denoted by $\mathbf{x} = [\theta_1, \omega_1, \theta_2, \omega_2, \theta_3, \omega_3]^{\mathrm{T}}$. Also, we assume that Assumptions 1–5 are satisfied in our MG model, and thus the power-flow balance in the network is represented by the DC power flow; see Sec. 2.3.

Under a multiplicative attack on the voltage measurement V_2 at DIC_2, we estimate the probabilistic worst-case bounds on all DIC frequencies. We model the attack on the voltage measurement of the DIC_2, denoted by $\boldsymbol{\xi} = \Delta V_2$, as a normally distributed random variable with zero mean and the standard deviation $\sigma_2 = 0.5$. Thus, the voltage measurement is scaled by the attack as in (8). Consequently, the power injection calculation P_2 is maliciously corrupted from the true sample value. Subsequently, we evaluate (11) to get the sensitivity variable $\boldsymbol{\Phi}$ in (10) at each time t as

$$\boldsymbol{\Phi} = \left[\frac{\partial\theta_1}{\partial\Delta V_2}, \frac{\partial\omega_1}{\partial\Delta V_2}, \frac{\partial\theta_2}{\partial\Delta V_2}, \frac{\partial\omega_2}{\partial\Delta V_2}, \frac{\partial\theta_3}{\partial\Delta V_2}, \frac{\partial\omega_3}{\partial\Delta V_2}\right]^{\mathrm{T}}.$$

Matrices and vectors required for the sensitivity equations (11) are given by

$$\boldsymbol{\Lambda}_{\mathbf{x}} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -\frac{\tilde{\omega}_1(\sum_{i=2}^{3} B_{ii})}{D_1} & -\tilde{\omega}_1 & \frac{\tilde{\omega}_1 B_{22}}{D_1} & 0 & \frac{\tilde{\omega}_1 B_{33}}{D_1} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ \frac{\tilde{\omega}_2 B_{22}}{D_2} & 0 & -\frac{\tilde{\omega}_2 B_{22}}{D_2} & -\tilde{\omega}_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ \frac{\tilde{\omega}_3 B_{33}}{D_3} & 0 & 0 & 0 & -\frac{\tilde{\omega}_3 B_{33}}{D_3} & -\tilde{\omega}_3 \end{bmatrix},$$

$$\boldsymbol{\Lambda}_{\boldsymbol{\xi}} = \left[0, 0, 0, -\frac{\tilde{\omega}_2 P_2}{D_2}, 0, 0\right]^{\mathrm{T}},$$

where both $\boldsymbol{\Lambda}_{\mathbf{x}}$ and $\boldsymbol{\Lambda}_{\boldsymbol{\xi}}$ are evaluated at $\boldsymbol{\xi} = \mathbf{0}$. With the nominal values of the frequency calculated by solving the reduced-order dynamic equations of the MG, we can determine probabilistic worst-case bounds on all DIC frequencies by following the equation in (13).

Fig. 6 shows the results of the estimated bounds for all DIC frequencies. In each part of the figure, upper and lower bounds (denoted by red and blue lines) are plotted for different confidence levels (i.e., 99.7%, 95%, and 68%, corresponding to 1, 2, and 3 standard deviations) with black dotted lines representing nominal trajectories without the attack. Green lines are trajectories obtained from 100 Monte Carlo simulations of the original nonlinear MG model with fully detailed DIC dynamics. Compared to the repeated simulation results, we can verify that the estimated bounds on the frequency of the proposed method accurately describe the worst-case system dynamics due to the potential attack. The bound estimate is instrumental for providing countermeasures by facilitating DER coordination under adversarial environments. Our approach supports use cases involving multi-microgrid environments, in which peer MGs with some interconnecting tie lines and a power sharing agreement can support critical loads in response to an adverse condition. For example, we consider the two-MG system shown in Fig. 7. Both MGs have a main MG bus and a critical load bus, with normally open inter-ties between these buses. We assume that the systems are in island mode. The reachability analysis indicates that an unsafe state is reachable because of a likely voltage attack at the DIC on the critical load bus in MG 1 (Event 1 and 2). We let the MG controllers exchange messages, with our implementation eventually using OpenFMB/DDS[1] [34].

[1]OpenFMB is an emerging grid edge communication standard to enable grid edge interoperability. Another research thrust of the project that supports the work described in the present paper is considering OpenFMB communications across local area networks (for example, between peer microgrids) over software-defined networks (SDN). The eventual goal of the work is to unify the reachability analysis, frequency stabilization, and secure inter-microgrid OpenFMB messaging as an OpenFMB use case.

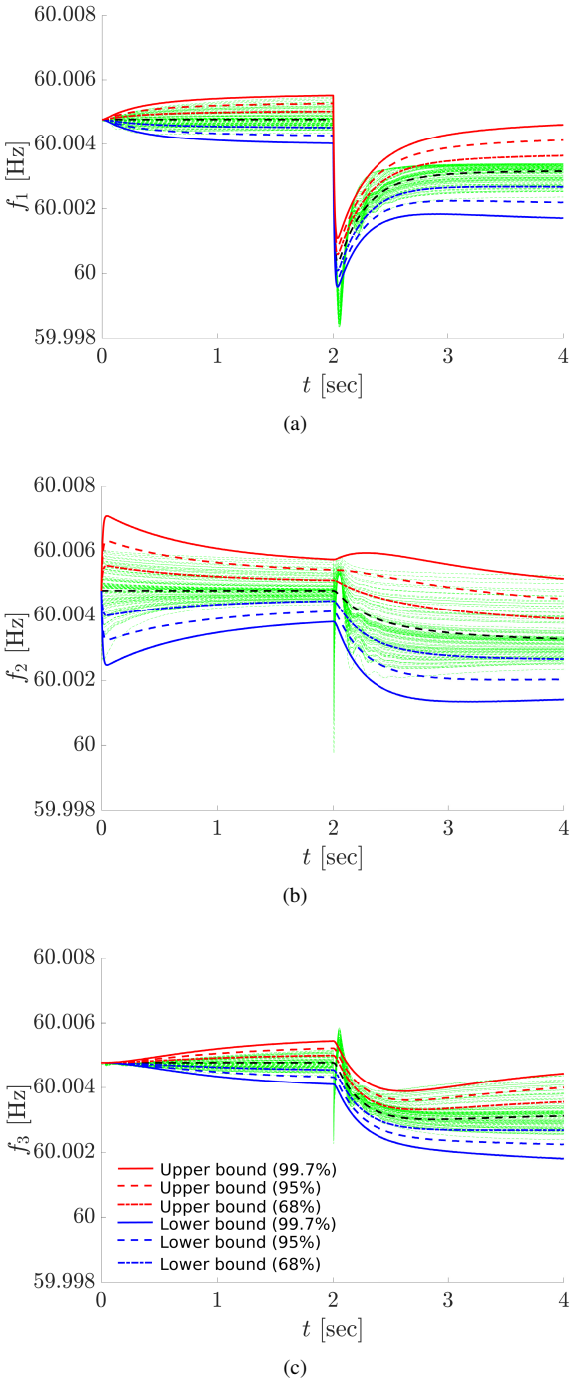

Figure 6. Simulation results of the MG are plotted for frequencies at DIC buses 1–3 (figures (a)–(c), respectively). Upper and lower bounds for different confidence levels are denoted by red and blue lines. Nominal trajectories (i.e., without any attack) are represented by black dotted lines. Green lines are the results from 100 repeated simulations based on the original fully detailed MG model.

Table 1. Computation Time for different network sizes.

Case	Number of DICs	Number of attacks	Computation time [s]
13 Bus	3	2	0.02
34 Bus	9	6	0.04
123 Bus	30	10	0.23
		25	1.1

In response to the reachability analysis (Event 2), the controllers reach consensus to close the tie line, and MG 1 trips off the faulted DER. The secondary frequency control algorithm quickly stabilizes the now connected two-MG system (Event 3).

In addition, the result proves that our approach is computationally efficient compared to other methods based on repeated numerical simulations such as Monte Carlo methods. Computation for the bound estimation took 0.0286 s for a 2 s interval to estimate the worst-case probabilistic bounds. Computing the Monte Carlo simulation over the same interval required 2200 s on a 2.53 GHz Intel® Processor, demonstrating that our proposed method has computational advantages over repeated numerical simulations and can be implemented in a nearly online fashion. To further validate the scalability of the proposed reachability analysis for large MGs, we compare computation times of a 2 s interval for estimating probabilistic bounds under different IEEE distribution feeder test cases (i.e., 13-bus, 34-bus, and 123-bus with arbitrary DIC locations), as shown in Table 1. Note that computation time increases with the network size and the number of attacks. As a MG typically consists of a few buses and DICs, these results show that the proposed method is suitable for nearly real-time MG stability-monitoring applications.

However, our method leads to over estimation in some cases (as shown in Fig. 6(a)), mainly because of errors from the linear approximation in (10). Also, some of the large transients at $t = 2$ s (reflecting load step-change) are not effectively captured by the bounds as a consequence of the simplified assumptions of our MG model. To improve the accuracy, we can incorporate higher-order terms in the analysis as discussed in [33, 35], adopt more accurate MG models (refer to different reduced-order DIC models in [21]), and consider the original nonlinear power-flow equations to capture the accurate transient phenomena at the cost of computational resources.

5. Conclusions and Future Work

In this paper, we focused on developing a systematic framework to analyze the cybersecurity

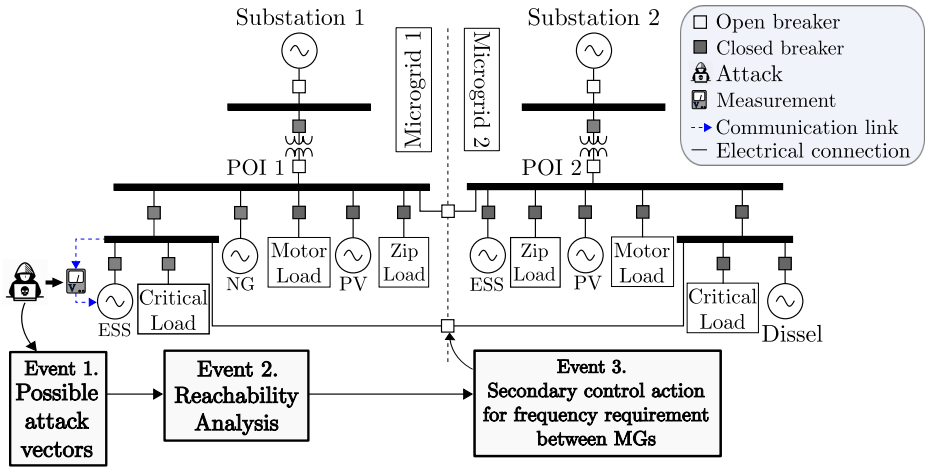

Figure 7. One-line diagram and sequence of operations for the two-MG system under a potential malicious attack.

impact on a microgrid in the presence of malicious attacks on measurement and control commands. We proposed a computationally efficient method to estimate probabilistic worst-case bounds on dynamic states under potential attacks. In addition, we were able to achieve computational advantages over exhaustive simulation-based methods, while accurately describing the worst-case system behavior. Consequently, we anticipate that the proposed approach will be useful in multiple contexts, e.g., in online stability monitoring against cyber attacks and in providing advisory information to microgrid operators to effectively coordinate DERs in a system.

The remaining shortcomings of our method include over estimated results due to errors from the linear approximation and failures to capture large transients of the dynamics as a result of the simplified microgrid model. To address those challenges in our future work, we plan to incorporate higher-order terms in the approximation and adopt different levels of model-order reduction to improve the accuracy of the analysis while minimizing computational burden. Furthermore, we will validate the performance of the event sequence introduced in Fig. 7 with a real-time simulator while extending our analysis by introducing new elements, such as protection devices and other hierarchical control schemes (e.g., secondary frequency control).

Appendix

A. Derivation of Sensitivity Equations

Assume that the network dynamics in (7) are continuously differentiable with respect to $(\mathbf{x}, \boldsymbol{\xi})$, and that there exists a unique solution for the nominal states, $x_i(t, \mathbf{0})$, at each instance. Then the solution of the ith state for a given $\boldsymbol{\xi}$ is given as:

$$x_i(t, \boldsymbol{\xi}) = x_i(t_0, \mathbf{0}) + \int_{\tau=t_0}^{t} f_i(\mathbf{x}, \boldsymbol{\xi}) d\tau. \tag{14}$$

Taking partial derivatives of (14) in terms of ξ_j, we have:

$$\frac{\partial x_i}{\partial \xi_j} = \int_{\tau=t_0}^{t} \sum_{k=1}^{m} \frac{\partial f_i}{\partial x_k} \frac{\partial x_k}{\partial \xi_j} + \frac{\partial f_i}{\partial \xi_j} \, d\tau. \tag{15}$$

By taking a derivative of (15) in terms of t, we get:

$$\frac{d}{dt}\phi_{ij} = \sum_{k=1}^{m} \frac{\partial f_i}{\partial x_k}\Big|_{\boldsymbol{\xi}=\mathbf{0}} \phi_{ij} + \frac{\partial f_i}{\partial \xi_j}\Big|_{\boldsymbol{\xi}=\mathbf{0}} \tag{16}$$

Collecting (16) $\forall i, j$, we can express the compact matrix form shown in (11).

References

[1] B. Lasseter, "Microgrids [distributed power generation]," in *Proc. 2001 IEEE Power Engineering Society Winter Meeting*, pp. 146–149.

[2] P. Borazjani, N. I. A. Wahab, H. B. Hizam, and A. B. C. Soh, "A review on microgrid control techniques," in *Proc. 2014 IEEE Innovative Smart Grid Technologies - Asia*, pp. 749–753.

[3] H. J. Liu, L.-Y. Lu, Z. Wu, and A. Valdes, "Distributed optimization approach for frequency control with emulated virtual inertia in islanded microgrids," in *Proc. Innovative Smart Grid Technologies Asia*, 2018.

[4] H. J. Liu, W. Shi, and H. Zhu, "Distributed voltage control in distribution networks: Online and robust implementations," *IEEE Trans. Smart Grid*, 2016, (Early Access).

[5] ——, "Hybrid voltage control in distribution networks under limited communication rates," *IEEE Trans. Smart Grid*, 2016, (Early Access).

[6] Z. Wu, W. Gao, T. Gao, W. Yan, H. Zhang, S. Yan, and X. Wang, "State-of-the-art review on frequency response of wind power plants in power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 1, pp. 1–16, Jan. 2018.

[7] H. F. Habib, C. R. Lashway, and O. A. Mohammed, "On the adaptive protection of microgrids: A review on how to mitigate cyber attacks and communication failures," in *Proc. 2017 IEEE Industry Applications Society Annual Meeting*, pp. 1–8.

[8] B. Chen, K. L. Butler-Purry, S. Nuthalapati, and D. Kundur, "Network delay caused by cyber attacks on SVC and its impact on transient stability of smart grids," in *Proc. 2014 IEEE PES General Meeting*, pp. 1–5.

[9] R. Lee, M. Assante, and T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *E-ISAC*, March 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[10] H. J. Liu, M. Backes, R. Macwan, and A. Valdes, "Coordination of DERs in microgrids with cybersecure resilient decentralized secondary frequency control," in *Proc. Hawaii International Conference on System Sciences*, 2018. [Online]. Available: http://hdl.handle.net/10125/50226

[11] L. Y. Lu, H. J. Liu, and H. Zhu, "Distributed secondary control for isolated microgrids under malicious attacks," in *Proc. IEEE North American Power Symposium*, 2016, pp. 1–6.

[12] V. Venkataramanan, A. Srivastava, and A. Hahn, "Real-time co-simulation testbed for microgrid cyber-physical analysis," in *Proc. 2016 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, pp. 1–6.

[13] M. Chlela, G. Joos, M. Kassouf, and Y. Brissette, "Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks," in *Proc. 2016 IEEE Power and Energy Society General Meeting*, pp. 1–5.

[14] V. Venkataramanan, P. Wang, A. Srivastava, A. Hahn, and M. Govindarasu, "Interfacing techniques in testbed for cyber-physical security analysis of the electric power grid," in *Proc. 2017 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, pp. 1–6.

[15] R. Macwan, C. Drew, P. Panumpabi, A. Valdes, N. Vaidya, P. Sauer, and D. Ishchenko, "Collaborative defense against data injection attack in IEC61850 based smart substations," in *Proc. 2016 IEEE Power and Energy Society General Meeting*, pp. 1–5.

[16] Z. Li and M. Shahidehpour, "Defense-in-depth framework for microgrid secure operations against cyberattacks," in *Proc. 2017 IEEE Power Energy Society General Meeting*, pp. 1–5.

[17] B. Chen, S. Mashayekh, K. L. Butler-Purry, and D. Kundur, "Impact of cyber attacks on transient stability of smart grids with voltage support devices," in *Proc. 2013 IEEE Power Energy Society General Meeting*, pp. 1–5.

[18] A. Farraj, E. Hammad, and D. Kundur, "On the impact of cyber attacks on data integrity in storage-based transient stability control," *IEEE Trans. Industrial Informatics*, vol. 13, no. 6, pp. 3322–3333, Dec. 2017.

[19] X. Liu, M. Shahidehpour, Y. Cao, L. Wu, W. Wei, and X. Liu, "Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330–1339, May 2017.

[20] K. J. Timko, A. Bose, and P. M. Anderson, "Monte Carlo simulation of power system stability," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-102, no. 10, pp. 3453–3459, Oct. 1983.

[21] A. Olaoluwapo, A. D. Domínguez-García, and P. Sauer, "A hierarchy of models for inverter-based microgrids," *Coordinated Science Lab tech report UILU-ENG-17-2201, University of Illinois at Urbana-Champaign*, May 2017. [Online]. Available: https://www.ideals.illinois.edu/handle/2142/96001

[22] B. Stott, J. Jardim, and O. Alsac, "DC power flow revisited," *IEEE Trans. Power Systems*, vol. 24, no. 3, pp. 1290–1300, Aug. 2009.

[23] J. W. Simpson-Porco, F. Dörfler, and F. Bullo, "Synchronization and power sharing for droop-controlled inverters in islanded microgrids," *Automatica*, vol. 49, no. 9, pp. 2603–2611, Sep. 2013.

[24] M. Zholbaryssov and A. D. Domínguez-García, "Distributed enforcement of phase-cohesiveness for frequency control of islanded inverter-based microgrids," *IEEE Trans. Control Netw. Syst.*, 2018, to be published.

[25] F. Dörfler, J. Simpson-Porco, and F. Bullo, "Breaking the hierarchy: Distributed control & economic optimality in microgrids," *IEEE Trans. Control Netw. Syst.*, vol. 3, no. 3, pp. 241–253, Sep. 2016.

[26] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodriguez, "Control of power converters in AC microgrids," *IEEE Power Electron. Lett.*, vol. 27, no. 11, pp. 4734–4749, Nov. 2012.

[27] S. T. Cady, A. D. Domínguez-García, and C. N. Hadjicostis, "A distributed generation control architecture for islanded AC microgrids," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 5, pp. 1717–1735, Sep. 2015.

[28] H. Han, X. Hou, J. Yang, J. Wu, M. Su, and J. M. Guerrero, "Review of power sharing control strategies for islanding operation of AC microgrids," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 200–215, Jan. 2016.

[29] C. Zhao, U. Topcu, N. Li, and S. Low, "Design and stability of load-side primary frequency control in power systems," *IEEE Trans. Autom. Control*, vol. 59, no. 5, pp. 1177–1189, May 2014.

[30] P. Anderson and A. Fouad, *Power System Control and Stability*, 2nd ed. Wiley India Pvt. Limited, 2008. [Online]. Available: https://books.google.com/books?id=2BXOzA34qBkC

[31] F. Dörfler and F. Bullo, "Kron reduction of graphs with applications to electrical networks," *IEEE Trans. Circuits Syst. I*, vol. 60, no. 1, pp. 150–163, Jan. 2013.

[32] H. Zhu and H. J. Liu, "Fast local voltage control under limited reactive power: Optimality and stability analysis," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3794–3803, Sep. 2016.

[33] H. Choi, P. J. Seiler, and S. V. Dhople, "Propagating uncertainty in power-system DAE models with semidefinite programming," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3146–3156, Jul. 2017.

[34] "Open field message bus," https://openfmb.github.io, accessed: 2018-09-04.

[35] H. Choi, P. J. Seiler, and S. V. Dhople, "Propagating uncertainty in power flow with the alternating direction method of multipliers," *IEEE Trans. Power Syst.*, vol. 33, no. 4, pp. 4124–4133, 2017.